A User Authentication Scheme of IoT Devices using Blockchain-Enabled Fog Nodes

Vrunda Paunikar[1] Nikita Paunikar[2] Vaishnavi Dewalkar[3] Neha Tambekar[4] Roshani Dighore[5]
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]K.D.K. College of Engineering, Umrer, India

Abstract— The main objective of this project is securely store and maintain the data using block chain. The blockchain technology is used to protect the healthcare data hosted within the cloud. The block that contain the data and the timestamp. It allows healthcare provider to access the IOT data more securely from anywhere. We propose a user authentication scheme using block chain-enabled fog nodes in which fog nodes interface to Ethereum smart contracts to authenticate users to access IoT devices. Block chain is fundamentally a decentralized, distributed, shared, and immutable database ledger that stores registry of assets and transactions across peer-to-peer (P2P) network. It preserve data from attackers. The data is encrypted prior to outsourcing to the cloud. The healthcare provider have to decrypt the data prior to download.

Keywords: IoT Devices, User Authentication Scheme

I. INTRODUCTION

IoT devices are being deployed at a massive scale, with Cisco forecaste 20 billion devices by the year 2020. As opposed to endpoint devices, IoT devices are assets constrained devices, and are incapable of securing and defending themselves, and can be easily hacked and compromised. Therefore, it is important to adopt proper schemes for verification and control access to ensure the overall security for IoT devices, their communications, and their data Any proper user authentication scheme to IoT devices must consider the fact that IoT devices are lack of resource devices and not able to carry through heavy processing and calculation. Also the authentication scheme must be reliable, extensible, and secure against known attacks and threats. Furthermore, fog computing has emerged as a new computing paradigm that has the ability to perform localized processing, storage, and analytics for a group of IoT devices. Many IoT solutions have now been put forth by researchers in make use of the fog nodes to relieve IoT devices from some of the heavy processing computational workload. Moreover, research communities as a distributive technology that is poised to play a major role in managing, controlling, and most importantly securing IoT devices. Blockchain can be a key enabling technology for providing feasible security solutions to today's challenging IoT security problems. To date, most authentication techniques for IoT systems are centralized in drawing and deployment, and rely on a Trusted Third Party to authenticate the entities such as Open Authorization (OAuth) protocol. This approach has disadvantages such as high cost, being a single point of failure, hacking, and privacy evasion. To overcome the drawbacks of the centralized based authentication, a decentralized authentication scheme using fog nodes and blockchain technology is proposed in this paper. This scheme facilitates controlling and accessing IoT devices while providing security without the need of a Trusted Third Party. Additionally, the proposed work includes the use of new architectures including edge determine and block chain, which applicable performing authentication at scale, by taking advantage of fog node deployment. The primary goal of this paper is to propose and analyze the security of a blockchain-based authentication scheme at scale

For IoT devices. Specifically, we present an architecture and design of a system involving end users, IoT devices, fog and cloud nodes, as well as Ethereum Blockchain smart contracts which rule the authentication rules and logic. The primary contributions of this paper can be summarized as follows: We propose a desperse and scalable authentication mechanism that utilizes blockchain-enabled fog nodes with connectivity to Ethereum smart contracts for authenticating user gain to IoT devices whereby access tokens are issued by the smart contracts with no intermediary or trusted third party.

II. LITERATURE REVIEW

E. Stefanov, C. Papamanthou, and E. Shi Dynamic Searchable Symmetric Encryption (DSSE) Enables a client to encrypt his document collection in a way that it is still searchable and efficiently updatable. We propose the first DSSE scheme that achieves the best of both worlds, i.e., both small leakage and efficiency. Our scheme leaks significantly less information than any other previous DSSE construction and supports both updates and searches in sub-linear time in the worst case, maintaining at the same time a data structure of only linear size. We finally provide an implementation of our construction, showing its practical efficiency

W. Ogata and K. Kurosawa A generic method to transform any SSE scheme (that is only secure against passive adversaries) to a no-dictionary verifiable SSE scheme. A client encrypts a set of files and an index table by a symmetric encryption scheme, and then stores them on an untrusted server. In the search phase, he can efficiently retrievethe matching files for a search keyword w keeping the keyword and the files secret.

M. Azraoui, K. Elkhiyaoui, M. Onen, and R. Molva Recent technological developments in cloud computing and the ensuing commercial appeal have encouraged companies and individuals to outsource their storage and computations to powerful cloud servers. We focus in particular on the scenario where a data owner wishes to outsource its public database to a cloud server; enable anyone to submit multi-keyword search queries to the outsourced

D. He et al. A new framework for the handshake scheme in MHSNs, which is based on hierarchical identity-based cryptography. We then construct an efficient Cross-Domain HandShake (CDHS) scheme that allows symptoms-matching within MHSNs. For example, using the proposed

CDHS scheme, two patients registered with different healthcare centers can achieve mutual authentication and generate a session key for future secure communications.

III. EXISTING SYSTEM

The two most popular types of mutual verification are certificate based verification and username/password based verification a group verification protocol where the created keys are shared among multiple nodes. However, executing key sharing and collective verification among multiple nodes puts them at risk if one of the nodes was compromised.

Disadvantages

- Storing the cryptographic credentials at the edge nodes exposes the protocol to cloning attacks
- While these techniques provide authentication for IoT devices, but notable limitations arise from being a centralized architecture.
- With a centralized architecture, the system becomes limited in terms of scalability, reliability, and also security as it becomes a single point of attack and compromise.

IV. PROPOSED SYSTEM

To overcome the security problems that are take place in the existing system and effectively store the data over the cloud we introduce this system.

Every transaction in the register is digital signed and validated by tens of thousands of mining nodes in the network.

Transactions are stored and organized by time stamps in groups called blocks. These blocks are linked (or chained) together to form a chain of blocks, or a block chain. The block chain uses AES scheme to provide strong cryptographic proof for data authentication and integrity.

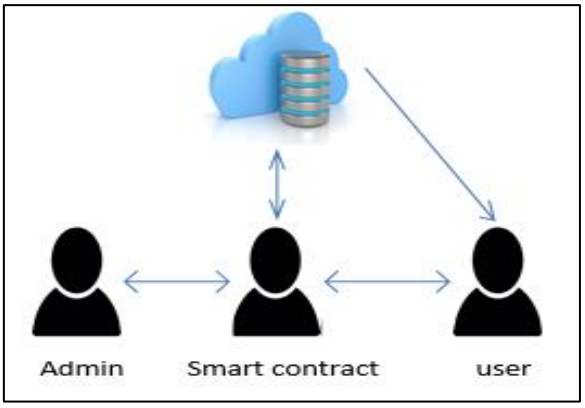
V. ADVANTAGES

- The data's are highly secured.
- The advent of the Ethereum block chain, which implements smart contracts, the potential use space for block chain has become endless.
- Confidentiality requirement is achieved by preventing unauthorized access to the IoT device and its data
- Integrity and non-repudiation are two significant security requirements that are needed in any IoT system to avoid data modification in addition to verify the sender identity.

VI. OBJECTIVE

- The main objective is to ensure the data security.
- To enable access control that is cryptographically increase.
- To ensure the protection of cloud database.
- To perform secure and efficient data retrieval.

VII. SYSTEM ARCHITECTURE



VIII. IMPLEMENTATION

A. User Authentication

User authentication is a process that allows a device to verify the identity of someone who connects to a network assets. There are many technologies currently present to a network administrator to authenticate users

B. File Upload

Uploading is the communication of a file from one computer system to another, usually larger computer system.
From a network user's opinion, to upload a file is to send it to another computer that is set up to receive it.

C. Admin Access

Admins are entities responsible for managing he user access control list and permissions for uploaded file. We assume there can be multiple admins for a particular enterprise or organization with management control. The main task of the admins is to manage registering and de-registering of uploaded file and fog nodes in the system.

D. Smart Contract

A single smart contract is used in our proposed solution for the whole system. The smart contract contains a plot of all the registered fog nodes and their related uploaded file they manage. Moreover, it contains a list of authenticated end users mapped to uploaded file they allowed to access. All registration, authentication, access control functionalities are governed in a distribute manner through the smart contract.

E. Encrypt File and Block Creation

The data is encrypted for secure maintenance. So that the unauthorized person cannot be able to access the data that are presented in the cloud. Each block contain patient record and its timestamp. A block chain, originally block is a growing list of records called blocks.

F. Key Generation

Key management refers to mainframe of cryptographic keys in a cryptosystem. This includes concerns with the generation, exchange, storage, use, crypto-destruction and replacement of keys.

It includes cryptographic protocol design, key servers, user procedures, and other applicable protocols.

Key management dealing keys at the user level, either between users or systems. This is in contrast to key scheduling, which typically refers to the internal conduct of keys within the action of a cipher.

G. File Download

Computing services will be suitable to encrypt documents to keep them safe in the cloud

Data search is the process of searching the data in a cloud

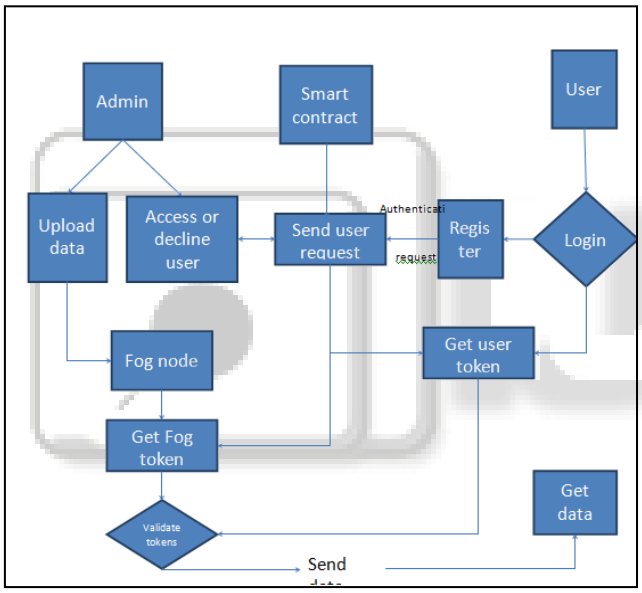
Getting the key is the only way to get the decrypted file. If not they will only get the encrypted file.

In this module user can search for their uploaded file which is stored in the cloud.

They will get the decrypted file after the key generated by the AES in the server.

In this module, Authentication of the key is being processed, after completion of the successful authentication the file is retrieved from the server in a decrypted form.

IX. Flow Diagram



X. Conclusion

We have proposed a system design, and implementation of a Block chain-based solution using Ethereum smart contracts for IoT devices authentication at scale, in a decentralized manner with no intermediary third party. We implemented the proposed Ethereum smart contract. Authenticating large scale of IoT devices is featured by involving fog nodes which are used to relieve the IoT devices from the processing burden of carrying out authentication tasks and the connectivity overhead involved with interfacing with the Ethereum Block chain network.

Reference

[1] S. Z. Syed Idrus, E. Cherrier, C. Rosenberger, and J.-J. Schwartzmann, "A review on authentication methods," vol. 7, pp. 95–107, 06 2013.

[2] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395 – 411, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17315765 L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," pp. 254–269, 10 2016.

[3] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," CoRR, vol. abs/1802.04410, 2018. [Online]. Available: http://arxiv.org/abs/1802. 04410

[4] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "Iot-oas: An auth-based authorization service architecture for secure services in Iot scenarios," IEEE Sensors Journal, vol. 15, no. 2, pp. 1224–1234, Feb 2015.

